EDUSUM

#1 Online Certification Guide

ISACA CCOA

ISACA Cybersecurity Operations Analyst Certification Questions & Answers

Exam Summary – Syllabus –Questions

CCOA

ISACA Certified Cybersecurity Operations Analyst (CCOA)

140 Questions Exam – 450/800 Cut Score – Duration of 240 minutes

Table of Contents:

Know Your CCOA Certification Well:

The CCOA is best suitable for candidates who want to gain knowledge in the ISACA Cybersecurity. Before you start your CCOA preparation you may struggle to get all the crucial Cybersecurity Operations Analyst materials like CCOA syllabus, sample questions, study guide.

But don't worry the CCOA PDF is here to help you prepare in a stress-free manner. The PDF is a combination of all your queries like-

- What is in the CCOA syllabus?
- How many questions are there in the CCOA exam?
- Which Practice test would help me to pass the CCOA exam at the first attempt?

Passing the CCOA exam makes you ISACA Certified Cybersecurity Operations Analyst (CCOA). Having the Cybersecurity Operations Analyst certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISACA CCOA Cybersecurity Operations Analyst Certification Details:

Exam Name	ISACA Certified Cybersecurity Operations Analyst (CCOA)
Exam Code	CCOA
Exam Price	ISACA Member: $399 (USD)
Exam Price	ISACA Non-member: $499 (USD)
Duration	240 mins
Number of Questions	140
Passing Score	450/800
Books / Training	CCOA Online Review Course
Schedule Exam	Exam Registration
Sample Questions	ISACA CCOA Sample Questions
Practice Exam	**ISACA CCOA Certification Practice Exam**

CCOA Syllabus:

Topic	Details	Weights
TECHNOLOGY ESSENTIALS	- Identify the key components of computer and cloud networking, understand how databases, virtualization, and containerization are leveraged, and become familiar with command-line interfaces, programming, scripting, and more. **A. NETWORKING** • Cloud Networking • Computer Networking • Devices, Ports, and Protocols • Network Access • Network Tools • Network Topology • Segmentation (Logical, Physical) **B. SYSTEMS/ENDPOINT** • Databases • Command Line • Containerization/Virtualization • Middleware • Operating Systems **C. APPLICATIONS** • Application Programming Interface (API) • Automated Deployment • Cloud Applications • Scripting/Coding	25%
CYBERSECURITY PRINCIPLES AND RISK	- Understand cybersecurity governance and alignment with business drivers, define cybersecurity strategy based on enterprise objectives, establish effective cross-organizational communication for cybersecurity and more. **A. CYBERSECURITY PRINCIPLES** • Compliance • Cybersecurity Objectives • Governance • Risk Management • Roles and Responsibilities • Cybersecurity Models **B. CYBERSECURITY RISK**	20%

Topic	Details	Weights
	• Application Risk • Cloud Technology Risk • Data Risk • Network Risk • Supply Chain Risk • System/Endpoint Risk • Web Application Risk	
ADVERSARIAL TACTICS, TECHNIQUES, AND PROCEDURES	- Understand common adversarial tactics, techniques, and procedures (TTPs), develop critical and creative thinking skills for threat detection and response, differentiate between dashboard events, attacker mindset insights and more. **A. THREAT LANDSCAPE** • Attack Vectors • Threat Actors/Agents • Threat Intelligence Sources **B. MEANS AND METHODS** • Attack Types • Cyber Attack Stages • Exploit Techniques • Penetration Testing	10%
INCIDENT DETECTION AND RESPONSE	- Understand the importance of cybersecurity-incident preparedness, recognize the significance of incident detection and response in mitigating their impact, appreciate the role of proactive planning, practice, process refinement and more. **A. INCIDENT DETECTION** • Data Analytics • Detection Use Cases • Indicators of Compromise and/or Attack • Logs and Alerts • Monitoring Tools and Technologies **B. INCIDENT RESPONSE** • Incident Containment • Incident Handling • Forensic Analysis • Malware Analysis • Network Traffic Analysis • Packet Analysis	34%

Topic	Details	Weights
	• Threat Analysis	
SECURING ASSETS	- Understand the importance of designing countermeasures to protect digital assets, recognize the iterative nature of securing systems and their ecosystems, appreciate the holistic approach to securing assets, consider technical aspects and organizational products, services and critical business processes, and more. **A. CONTROLS** • Contingency Planning • Controls and Techniques • Identity and Access Management • Industry Best Practices, Guidance, Frameworks, and Standards **B. VULNERABILITY MANAGEMENT** • Vulnerability Assessment • Vulnerability Identification • Vulnerability Remediation • Vulnerability Tracking	11%

ISACA CCOA Sample Questions:

Question: 1

Why is vulnerability tracking essential in cybersecurity operations?

a) To reduce DNS queries
b) To improve firewall throughput
c) To monitor status and ensure closure of issues
d) To bypass change management

Answer: c

Question: 2

Who is ultimately accountable for cybersecurity governance in an organization?

a) Security analyst
b) System administrator
c) CEO or board of directors
d) IT support staff

Answer: c

Question: 3

In the context of risk management, what is “residual risk”?

a) Risk with zero impact
b) Risk not yet identified
c) The likelihood of detection
d) Risk after controls are applied

Answer: d

Question: 4

Which factors contribute to cloud technology risk?

a) Poor identity and access management
b) Overprovisioning of compute resources
c) Lack of encryption in transit
d) Frequent service updates

Answer: a, c

Question: 5

An organization is developing a cybersecurity governance program. The board has asked for a framework that clearly defines roles and responsibilities, enforces alignment with compliance requirements, and supports long-term strategic planning.

Which actions should be prioritized to support this initiative?

a) Purchase an EDR solution immediately
b) Define risk appetite and tolerance thresholds
c) Assign formal cybersecurity roles and responsibilities
d) Implement automated threat detection tools
e) Align governance structure with a framework like NIST or COBIT

Answer: b, c, e

Question: 6

In which cyber-attack stage does lateral movement typically occur?

a) Initial access
b) Reconnaissance
c) Privilege escalation
d) Post-exploitation

Answer: d

Question: 7

What are two common challenges in vulnerability tracking? (Choose two)

a) Lack of prioritization
b) Excessive endpoint bandwidth
c) Poor documentation
d) Encryption of log files

Answer: a, c

Question: 8

During which stage of a cyberattack would a threat actor typically perform reconnaissance?

a) Command and control
b) Data exfiltration
c) Pre-attack
d) Initial access

Answer: c

Question: 9

Which of the following are risks associated with unpatched systems? (Choose two)

a) Improved system performance
b) Feature rollbacks
c) Exploitation of known vulnerabilities
d) Malware infections

Answer: c, d

Question: 10

Your organization has observed an increase in suspicious login attempts from international IPs. Threat intelligence indicates a campaign targeting multiple industries. The attackers use open-source tools and leverage known exploits to gain initial access.

What steps should your team take in response to this evolving threat landscape?

a) Subscribe to an industry-specific ISAC
b) Implement geo-IP blocking for non-business regions
c) Wait for law enforcement to respond
d) Enhance anomaly-based monitoring
e) Disable VPN access for all users

Answer: a, b, d

Study Guide to Crack ISACA Cybersecurity Operations Analyst CCOA Exam:

- Getting details of the CCOA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CCOA exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ISACA provided training for CCOA exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CCOA sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CCOA practice tests is must. Continuous practice will make you an expert in all syllabus areas.